



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,420	08/14/2001	John W.L. Ogilvie	1384.2.3D	1216

23484 7590 05/17/2004

JOHN W. L. OGILVIE
1320 EAST LAIRD AVENUE
SALT LAKE CITY, UT 84105

EXAMINER

AKPATI, ODAICHE T

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 05/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/929,420

Applicant(s)

OGILVIE, JOHN W.L.

Examiner

Tracey Akpati

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 2/23/04
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 19-53 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 19-53 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

DETAILED ACTION

1. Due to deficiencies in the Kudo et al (2001/0052071 A1) foreign priority date, this reference has been withdrawn, and replaced with Guski et al (5661807) and Chang et al (6105012). A new rejection can be found below.
2. *The attorney argues that Staheli et al fails to teach hiding of information.* Staheli et al teaches hiding of the data on column 5, lines 25-45. The message copy is stored at a replacement server and this server is not active until this copy is requested. Hence when the copy is stored, the copy is hidden from the public because the server that it is stored on is deactivated.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 19, 20, 27-31, 36-42 rejected under 35 U.S.C. 102(e) as being anticipated by Staheli et al (5537533).

With respect to Claim 19, the limitation “a computer system comprising a network, message storage means for storing in the network copies of a message, thereby hiding copies of sensitive information, and message disclosure means for disclosing the message if a predefined condition is detected” is met in the abstract and on column 4, lines 26-29.

With respect to Claim 20, the limitation “wherein the message storage means comprises an encryption means for encrypting at least one message component” is met on column 6, lines 2-3.

With respect to Claim 27, the limitation “wherein the network includes a local area network” is met on column 8, lines 53-55.

With respect to Claim 28, the limitation “wherein the network includes a geographically dispersed network and at least two copies of the message are geographically dispersed in the network” is met on column 5, lines 29-35, column 6, lines 65-67 and column 1, lines 40-43.

With respect to Claim 29, the limitation “wherein the network includes nodes on different continents and at least two copies of the message are stored on different continents in the network” is met on column 5, lines 29-35, column 6, lines 65-67 and column 1, lines 55-56.

With respect to Claim 30, the limitation “further comprising a means for changing the location of message copies” is met on column 5, lines 25-35.

With respect to Claim 31, the limitation “comprising a means for placing message copies in at least one file disguise” is met on column 1, lines 19-24, lines 65-67 and column 2, lines 1-14.

With respect to Claim 36, the limitation “comprising a message update storage means for storing message updates” is met on column 5, lines 29-32.

With respect to Claim 37, the limitation “wherein the message update storage means comprises code for creating decoy updates” is met on column 1, lines 19-24, 65-67 and column 2, lines 1-14.

With respect to Claim 38, the limitation “wherein the message update storage means comprises code for creating at least one secrecy renewal” is met on column 6, lines 2-3.

With respect to Claim 39, the limitation “wherein the message update storage means comprises code for creating at least one address marker” is inherent in column 5, lines 5-15.

With respect to Claim 40, the limitation “wherein the message update storage means comprises code for creating at least one searching update” is inherent on column 4, lines 59-63.

With respect to Claim 41, the limitation “wherein the message update storage means comprises code for creating at least one update to a roving message” is inherent on column 4, lines 59-63.

With respect to Claim 42, the limitation “wherein the message update storage means comprises code for creating at least one update to a poised message” is inherent on column 4, lines 59-63.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Staheli et al (5537533) in view of Chang et al (6134584).

With respect to Claim 24, Staheli et al meets all the limitation except the limitation described below.

The limitation "wherein the message disclosure means comprises a web page generator for creating and posting at least a portion of a web page containing a copy of at least a portion of the stored message" is met by Chang et al on column 3, lines 27-52.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chang et al within the system of Staheli et al because a web page generation is a common means of message sharing. An advantage of this method is that it is very convenient for all recipients to access the information disclosed. Hence, it would have been obvious to employ the teachings of Chang et al to Staheli et al to meet the claimed invention.

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Staheli et al (5537533) in view of Chang et al (6105012).

With respect to Claim 21, Staheli et al meets all the limitation except that described below.

The limitation “wherein the message storage means comprises a digital signature means for digitally signing at least one message component” is met by column 9, line 54 to column 10, line 20 of Chang et al.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chang et al within the system of Staheli et al because a digital signature is a common and well known method in the art for authenticating the message sent to the recipient.

Claim 46 is rejected under 35 U.S.C. 103(a) as being unpatentable over Guski et al (5661807) in view of Chang et al (6105012).

With respect to Claim 46, all the limitation is met by Guski et al except the limitation disclosed below.

The limitation of “wherein at least the sensitive information component is digitally signed” is met by column 9, line 54 to column 10, line 20 of Chang et al.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chang et al within the system of Guski et al because a digital signature is a well known method in the art of authentication of the sender of a message.

Claims 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Staheli et al (5537533) in view of Schmidt et al (6038689).

With respect to Claim 25, Staheli et al meets all the limitation except the limitation described below.

The limitation “wherein the message disclosure means comprises code for detecting a deadman switch for triggering disclosure” is met by Schmidt et al on column 4, lines 48-51.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Schmidt et al within the system of Staheli et al because a deadman switch is a useful step in working processes for triggering an emergency step when a precondition is met. Hence, it would have been obvious to employ this means in order to automate a process based on a precondition.

With respect to Claim 26, Staheli meets all the limitation except that disclosed below.

The limitation “wherein the message disclosure means comprises code for detecting a reverse deadman switch for triggering disclosure” is met by Schmidt et al on column 4, lines 48-51. It is obvious to have a reverse deadman switch from a deadman switch because this is just the same process but in reverse.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Schmidt et al within the system of Staheli et al because of the reason discussed in Claim 25 rejection.

Claims 32, 33, 34 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Staheli et al (5537533) in view of Brookes (5428778).

With respect to Claim 32, Staheli meets all the limitation except that described below.

The limitation "further comprising a message deletion means for deleting message copies" is met by Brookes on column 2, lines 66-68 and column 3, lines 1-5.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Brookes within the system of Staheli et al because the deletion of the secret message would prevent an attacker from being able to gain access to a message saved on the server in a remote location. Since the message will be deleted from all locations it is stored, it would prevent any form of message leakage to an outside party or to a curious administrator.

Hence it would have been obvious to employ the teachings of Brookes to the system of Staheli to meet the claimed invention.

With respect to Claim 33, Staheli meets all the limitation except that described below.

The limitation "wherein the message deletion means comprises a means for performing an emergency action in response to an apparent deletion request" is met by Brookes on column 2, lines 66-68 and column 3, lines 1-5.

It would have been obvious to one of ordinary skill in the art to combine the teachings of Brookes within the system of Staheli et al because of the reasons described in Claim 32 rejection.

With respect to Claim 34, Staheli meets all the limitation except that described below.

The limitation “wherein the message deletion means comprises a cancellation means for deleting all stored message copies” is met by Brookes on column 2, lines 66-68 and column 3, lines 1-5.

It would have been obvious to one of ordinary skill in the art to combine the teachings of Brookes within the system of Staheli et al because of the reasons described in Claim 32 rejection.

With respect to Claim 35, Staheli meets all the limitation except that described below.

The limitation “wherein the cancellation means requires authentication information which confirms that: the source of the cancellation request is the same as the source of the message to be canceled” is met by Brookes on column 5, lines 50-53 and column 6, lines 13-20.

It would have been obvious to one of ordinary skill in the art to combine the teachings of Brookes within the system of Staheli et al because it would make the system less prone to an attack by an intruder if an authenticating step was required before a cancellation request is allowed. If an attacker wanted to intentionally delete the owner's data, he would need to have some form of authenticating information belonging to the user such as a userid and password to be able to delete his information. Hence the requirement of this secret information enhances the security of the storage system.

Therefore, it would have been obvious to employ the teachings of Brookes to the system of Staheli to achieve the claimed invention.

Claim 43, 44, 47-50, 52, 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guski et al (5661807).

With respect to Claim 43, the limitation of “a signal embodied in a network for controlled message disclosure, the signal comprising a sensitive information component which is hidden in the network and a disclosure condition component” is met by Guski et al in the abstract and on column 3, lines 59-65. The sensitive information component is represented by the password. The password is sensitive information because it is confidential information. It is hidden in the network because after transformation, it is an undecipherable code (column 3, lines 35-37). It is in this transformed state that it is transmitted to the receiving host. Hence this password is hidden by its taking on the form of an undecipherable, encrypted code. The disclosure condition component is the time-dependent information. This is because the disclosure of the encrypted password is based on the condition that the comparison between the regenerated time-dependent information and reference time-dependent information available at the authenticating node is positive (see column 3, lines 26-34).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize the teachings of Guski et al to achieve the claimed invention because Guski et al discloses a system whereby a password, a sensitive information is hidden in a network through encryption and disclosed on the condition of a positive comparison between a regenerated time-dependent information and a reference time-dependent information at the authenticating node.

With respect to Claim 44 the limitation of “wherein at least the sensitive information component is encrypted” is met by Guski et al on column 3, lines 35-37.

With respect to Claim 47, the limitation “further comprising a destination component” is met by Guski et al on column 3, lines 55-58. The application ID represents the destination component because it identifies the host application being accessed (column 6, 29-30), and hence identifies the destination node.

With respect to Claim 48, the limitation “further comprising a disclosure format component” is inherently met by Guski et al on column 3, lines 2-8. The invertible transformation dictates the disclosure format of the password.

With respect to Claim 49, the limitation “further comprising an identification component” is met by Guski et al on column 3, lines 55-58. The user ID represents the identification component.

With respect to Claim 50, the limitation “further comprising a traveling program component” is met by Guski et al in the abstract. The password is a function of a non-time dependent value, a time-dependent value, all of which are combined and then transformed into an alphanumeric character string that is transmitted as a one-time password. This transformed password is hence the traveling program component.

With respect to Claim 52, the limitation “comprising code for monitoring conditions to determine if disclosure or deletion is appropriate” is met by Guski et al on column 3, lines 26-34.

The condition for disclosure is if a match occurs between the regenerated time-dependent information and reference time-dependent information.

With respect to Claim 53, the limitation "wherein the code operates independently of any message update signals" is met on by Guski et al on column 2, lines 1-8 and column 6, lines 20-25. The code, which is a one-time password, does not depend on any message update signals. This is because after the password is validated, it is never reused. Hence this doesn't give the system an opportunity to update the message/password with any update signals.

Claim 45 is rejected under 35 U.S.C. 103(a) as being unpatentable over Guski et al (5661807) in view of Staheli et al (5537533).

With respect to Claim 45, all the limitation is met by Guski et al except that described below.

The limitation "wherein at least the sensitive information component is compressed" is met by Staheli et al on column 6, lines 2-3.

It would have been obvious to one of ordinary skill in the art to combine the teachings of Staheli et al within the system of Guski et al because compression of the stored information will create more room for more data to be stored and consequently save storage space.

Claim 51 is rejected under 35 U.S.C. 103(a) as being unpatentable over Guski et al (5661807) in view of Brookes (5428778).

With respect to Claim 51, all the limitation is met by Guski et al except that described below.

The limitation "further comprising a deletion condition component" is met by Brookes on column 2, lines 66-68 and column 3, lines 1-5.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Brookes within the system of Guski et al because the deletion of the secret message would prevent an attacker from being able to gain access to a message saved on the server in a remote location. Since the message will be deleted from all locations it is stored, it would prevent any form of message leakage to an outside party or to a curious administrator.

Hence it would have been obvious to employ the teachings of Brookes to the system of Guski et al to meet the claimed invention.

Claims 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over unpatentable over Staheli et al (5537533) in view of Porter et al (6181781 B1).

With respect to Claim 22, all the limitation is met by Staheli et al except that described below.

The limitation "wherein the message storage means comprises code to send a notice to a specified email address after the message has been stored" is met by Porter et al on column 5, lines 33-61.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Porter et al within the system of Staheli et al because the sending of a message after storage is a common sanity check for alerting the sender that his message has been stored successfully.

With respect to Claim 23, all the limitation is met by Staehli et al except that described below.

The limitation "wherein the message disclosure means comprises an email message generator for creating and mailing at least one email message containing a copy of at least a portion of the stored message" is met by Porter et al on column 5, lines 52-60.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Porter et al within the system of Staheli et al because email is a common and reliable way of communicating a message to one or more message recipients. Hence it would be obvious to employ the teachings of Porter et al within the system of Staheli et al to obtain the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 703-305-7820. The examiner can normally be reached on 8.30am-6.00pm.

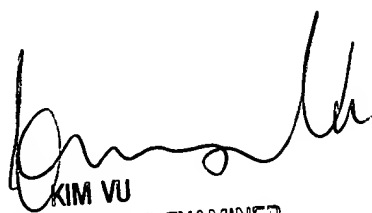
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone numbers for the

Art Unit: 2135

organization where this application or proceeding is assigned are 703-746-7240 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

OTA
May 5, 2004



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100